

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-134101

(P2003-134101A)

(43) 公開日 平成15年5月9日 (2003.5.9)

(51) Int.Cl. ⁷	識別記号	F I	データコード* (参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 9 C 1/00	6 5 0 Z 5 J 1 0 4
G 0 9 C 1/00	6 5 0	H 0 4 L 9/00	6 0 1 A
H 0 4 L 9/10			6 0 1 E
			6 2 1 A

審査請求 未請求 請求項の数18 O L (全 12 頁)

(21) 出願番号 特願2002-212912(P2002-212912)

(22) 出願日 平成14年7月22日 (2002.7.22)

(31) 優先権主張番号 特願2001-224126(P2001-224126)

(32) 優先日 平成13年7月25日 (2001.7.25)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72) 発明者 横田 薫
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 湯川 泰平
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100090446
弁理士 中島 司朗

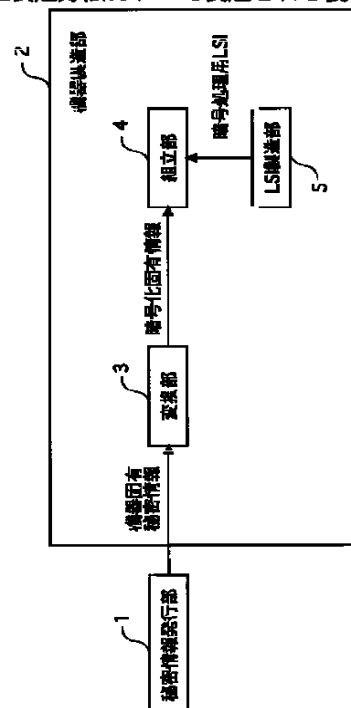
最終頁に続く

(54) 【発明の名称】 暗号処理用の素子とその暗号処理に用いる情報とを有する復号装置の製造方法、復号装置が有する情報と素子とを供給する供給システム、および前記製造方法において製造される復号装置。

(57) 【要約】

【課題】 復号鍵を用いて復号処理を施す復号装置を製造する場合に、組立部において復号鍵のセキュリティを管理する特殊な環境が必要である。本発明は、組立部において特殊な環境の不必要な製造方法を提供することを目的とする。

【解決手段】 変換部3において、セキュリティが管理された状態で、復号鍵を秘密に取得して、取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して出力する。組立部4において、出力された前記変換情報を前記復号装置に組み込まれるべき不揮発性メモリに書き込み、前記暗号化復号鍵に前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とが集積された1個の集積素子を含む前記復号装置を組み立てる。



【特許請求の範囲】

【請求項1】 復号鍵を用いて復号処理を施す復号装置の製造方法であって、
 セキュリティが管理された状態において、前記復号鍵を秘密に取得する取得ステップと、
 前記セキュリティが管理された状態において、取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して出力する変換情報出力ステップと、
 出力された前記変換情報を、前記復号装置に組み込まれるべき不揮発性メモリに書き込む書き込みステップと、
 前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とが集積された1個の集積素子を含む前記復号装置を組み立てる組み立てステップとを含むことを特徴とする製造方法。

【請求項2】 前記書き込みステップは、
 前記セキュリティが管理された状態よりもセキュリティレベルの低い状態で実施されることを特徴とする請求項1に記載の製造方法。

【請求項3】 前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、
 前記変換情報出力ステップは、
 所定の固定値の秘密鍵を用いて前記復号鍵に暗号処理を施すことを特徴とする請求項1に記載の製造方法。

【請求項4】 前記変換情報出力ステップは、
 複数種類の暗号処理から1個を選択して、前記所定の暗号処理とする選択サブステップと、前記選択サブステップにより選択された前記所定の暗号処理を示す選択情報を生成する選択情報生成サブステップと、
 前記復号鍵に前記所定の暗号処理を施して暗号化復号鍵を生成する暗号処理サブステップと、前記暗号化復号鍵と前記選択情報とを含む変換情報を生成する変換情報生成サブステップとを含み、
 前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むことを特徴とする請求項1に記載の製造方法。

【請求項5】 前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、
 前記選択サブステップは、
 複数の秘密鍵から1個の秘密鍵を選択し、
 前記選択情報生成サブステップは、
 選択された前記秘密鍵を示す選択情報を生成し、
 前記暗号処理サブステップは、
 選択された前記秘密鍵を用いて、前記復号鍵に暗号処理を施して暗号化復号鍵を生成し、
 前記変換情報生成サブステップは、
 前記暗号化復号鍵と前記選択情報とを含む変換情報を生成し、
 前記特定回路は、前記選択情報に基づいて、選択された

前記秘密鍵を特定することを特徴とする請求項4に記載の製造方法。

【請求項6】 前記変換情報出力ステップは、さらに、
 前記複数の秘密鍵を生成する鍵生成サブステップを含み、
 前記選択サブステップは、
 当該鍵生成サブステップにより生成された前記複数の秘密鍵から1個の前記秘密鍵を選択することを特徴とする請求項5に記載の製造方法。

【請求項7】 前記取得ステップは、
 復号装置毎に固有の復号鍵を取得することを特徴とする請求項1に記載の製造方法。

【請求項8】 復号装置に書き込まれる情報を供給する情報供給装置と、当該復号装置に組み込まれる集積素子を供給する集積素子供給装置とからなる供給システムであって、
 前記情報供給装置は、セキュリティの管理された状態で設けられ、
 前記復号装置において復号処理に用いられる復号鍵を秘密に取得する取得手段と、
 前記取得手段により取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して、当該変換情報を前記復号装置を組み立てる組立部に出力する変換情報出力手段とを備え、
 前記集積素子供給装置は、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と、当該復号鍵を用いて復号処理を施す回路とが集積された1個の集積素子を製造する製造手段と、前記製造手段により製造された集積素子を前記組立部に供給する集積素子供給手段とを備えることを特徴とする供給システム。

【請求項9】 前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、
 前記変換情報出力手段は、
 所定の固定値の秘密鍵を用いて前記復号鍵に暗号処理を施すことを特徴とする請求項8に記載の供給システム。

【請求項10】 前記変換情報出力手段は、
 複数種類の暗号処理から1個を選択して、前記所定の暗号処理とする選択手段と、
 前記選択手段により選択された前記所定の暗号処理を示す選択情報を生成する選択情報生成手段と、
 前記復号鍵に前記所定の暗号処理を施して暗号化復号鍵を生成する暗号処理手段と、
 前記暗号化復号鍵と前記選択手段とを含む変換情報を生成する変換情報生成手段とを含み、
 前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むことを特徴とする請求項8に記載の供給システム。

【請求項11】 前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、

前記選択手段は、
 複数の秘密鍵から1個の秘密鍵を選択し、
 前記選択情報生成手段は、
 選択された前記秘密鍵を示す選択情報を生成し、
 前記暗号処理手段は、
 選択された前記秘密鍵を用いて、前記復号鍵に暗号処理を施して暗号化復号鍵を生成し、
 前記変換情報生成手段は、
 前記暗号化復号鍵と前記選択手段とを含む変換情報を生成し、
 前記特定回路は、前記選択情報に基づいて、選択された前記秘密鍵を特定することを特徴とする請求項10に記載の供給システム。

【請求項12】 前記変換情報出力手段は、さらに、
 前記複数の秘密鍵を生成する鍵生成手段を含み、
 前記選択手段は、
 当該鍵生成手段により生成された前記複数の秘密鍵から1個の前記秘密鍵を選択することを特徴とする請求項11に記載の供給システム。

【請求項13】 前記取得手段は、
 復号装置毎に固有の復号鍵を取得することを特徴とする請求項8に記載の供給システム。

【請求項14】 復号鍵を用いて復号処理を施す復号装置であって、
 前記復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれている不揮発性メモリと、
 前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含む1個の集積素子とを備えることを特徴とする復号装置。

【請求項15】 前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、
 前記不揮発性メモリは、
 所定の固定値の秘密鍵を用いて、前記復号鍵に秘密鍵暗号方式の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれており、
 前記集積素子は、
 前記暗号化復号鍵に、前記秘密鍵を用いて復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含むことを特徴とする請求項14に記載の復号装置。

【請求項16】 前記不揮発性メモリは、
 複数種類の暗号処理から1個を選択して前記所定の暗号処理とし、選択された前記所定の暗号処理を示す選択情報と前記暗号化復号鍵とを含む変換情報が書き込まれており、
 前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むことを特徴とする請求項14に記載の復号装置。

【請求項17】 前記所定の暗号処理は、秘密鍵を用い

た秘密鍵暗号方式であり、
 前記不揮発性メモリは、
 複数の秘密鍵から1個の秘密鍵を選択し、選択された前記秘密鍵を示す選択情報と、前記秘密鍵を用いて秘密鍵暗号方式の暗号処理を施した暗号化復号鍵とを含む変換情報が書き込まれており、
 前記集積素子は、前記選択情報に基づいて、選択された前記秘密鍵を特定する前記特定回路を含むことを特徴とする請求項16に記載の復号装置。

【請求項18】 前記不揮発性メモリは、
 復号装置毎に固有の復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれていることを特徴とする請求項14に記載の復号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、著作権保護機能を持つAVデジタル機器などのように、暗号処理用の素子とその暗号処理に用いる情報とを有する復号装置の製造方法、復号装置が有する情報と素子とを供給する供給システム、および前記製造方法において製造される復号装置に関する。

【0002】

【従来の技術】近年、映画や音楽などのAVコンテンツのデジタル化が進み、映画や音楽などの有料コンテンツ配信サービスや、デジタル放送の限定放送といった各種サービスが実現されている。そういったサービスを実現するためには、配信あるいは放送するAVコンテンツに対して暗号処理を施して不正な視聴を防止する必要がある。例えば、AVコンテンツを記録媒体に記録させて配布する場合や、インターネットや放送網などによってAVコンテンツを配信する場合には、記録あるいは配信されるAVコンテンツは暗号化される。この暗号化されたAVコンテンツは、視聴料を払った特定のユーザまたは視聴者だけが復号化でき再生できる仕組みとなっている。

【0003】上記の仕組みを実現する再生機器は、暗号化されたコンテンツの復号化などを行うための暗号処理回路と鍵情報とを備える必要がある。このような再生機器の製造過程においては、通常のAVデコード機器の製造工程に加えて、暗号処理回路の製造、及び暗号処理に用いる鍵情報の書き込み、といった工程が必要である。

【0004】図7は記録媒体を利用した有料コンテンツ配布方式の構成を示す図である。有料コンテンツ記録媒体15は、例えば光ディスクといった大容量のデジタルコンテンツデータを記録できる記録媒体であり、暗号化コンテンツ鍵データを記録する暗号化コンテンツ鍵データ記録領域17と暗号化コンテンツデータを記録する暗号化コンテンツデータ記録領域18とを備える。暗号化コンテンツ鍵データは、有料コンテンツを購入したユーザが有する再生機器に固有の機器固有秘密情報を用い

て、コンテンツ鍵を暗号化することで得られ、暗号化コンテンツデータは、コンテンツ鍵データを用いてコンテンツデータを暗号化することで得られる。また、有料コンテンツ再生機器16は、有料コンテンツ記録媒体15に記録されている有料コンテンツデータを再生するための再生機器であり、暗号処理に必要な機器固有秘密情報を記録する不揮発性メモリ19と、有料コンテンツデータを復号化するための暗号処理を行う暗号処理用LSI20とを備える。ここで、機器固有秘密情報とは、機器ごとに固有な秘密情報として与えられるものである。有料コンテンツ再生機器16が、有料コンテンツ記録媒体15に記録されている有料コンテンツデータを再生する際の処理は以下の通りである。

【0005】まず、暗号処理用LSI20は、暗号化コンテンツ鍵データ記録領域17から暗号化コンテンツ鍵データ、そして暗号化コンテンツデータ記録領域18から暗号化コンテンツデータを読み出す。さらに暗号処理用LSI20が、不揮発性メモリ19に記録された機器固有秘密情報を用いて、一連の復号処理を行って暗号化コンテンツデータを復号化する。

【0006】有料コンテンツ再生機器16内において、暗号化コンテンツを復号化するには、コンテンツ鍵データが必要である。そのコンテンツ鍵データを復号化するには機器固有秘密情報が必要がある。したがって有料コンテンツを購入したユーザが所有する有料コンテンツ再生機器16だけが有料コンテンツを再生することができ、他のユーザの不正な再生が防止される。

【0007】図8はインターネットや放送網を利用した有料コンテンツ配信方式の構成を示す図である。図7の例で有料コンテンツ記録媒体15から読み出していた暗号化コンテンツ鍵データ及び暗号化コンテンツデータは、図8の例では有料コンテンツ配信局21の有料コンテンツ配信手段23から通信路を介して有料コンテンツ再生機器22に伝送される。有料コンテンツ配信局21は、インターネットを利用した有料コンテンツ配信の場合には、コンテンツプロバイダであり、放送網を利用した配信の場合には、放送局である。また、図8の場合の有料コンテンツ再生機器22は、有料コンテンツを購入したユーザが受信した有料コンテンツを再生するためのPCあるいはデジタルセットトップボックスなどのことである。暗号化コンテンツ鍵データ及び暗号化コンテンツデータを受信した後の処理は、図7の例における有料コンテンツ再生機器16の処理と同様である。

【0008】図9は図8の有料コンテンツ再生機器22に含まれる暗号処理用LSI25の内部構成を示す図である。暗号処理用LSI25はコンテンツ鍵復号回路251とコンテンツ復号回路252を含む。図9を用いて、暗号処理用LSI25の処理について説明する。まず、暗号化コンテンツ鍵復号回路251は、不揮発性メモリ24から読み出した機器固有秘密情報を用いて、外

部から入力される暗号化コンテンツ鍵データに対して所定の復号処理を行い、コンテンツ鍵を得る。そして、コンテンツ復号回路252は、そのコンテンツ鍵を用いて外部から入力される暗号化コンテンツデータを復号化する。

【0009】図10は不揮発性メモリと暗号処理用LSIとを備える有料コンテンツ再生機器の製造方法に関する従来の構成を示す図である。秘密情報発行部26は、有料コンテンツ再生機器に実装するための暗号技術の使用を機器製造部27に許可するライセンス機関により運営されている。秘密情報発行部26により発行された機器固有秘密情報は、秘密に、機器の製造を許可された機器製造部27に送付される。図10の機器製造部27は、組立部271とLSI製造部272とを備える。組立部271は、送付された機器固有秘密情報を、不揮発性メモリ24に書き込む。この不揮発性メモリ24は、LSI製造部272で製造された暗号処理用LSI25などと共に組立てられて、有料コンテンツ再生機器が製造される。なお、有料コンテンツ再生機器には、上記の他にAVコンテンツデータの復号などに必要な回路が組み込まれているが、それらは本発明とは直接関係がないのでここでは割愛している。

【0010】また、機器固有秘密情報は、不正利用を防止するため、発行されてから完成品として組み立てられるまで機密性が保持されなければならない。したがって組立部271において、施錠可能なドアと仕切りによって区切られた作業スペースを確保し、その中での作業者をごく限られた者だけに限定する等の措置が行われる。

【発明が解決しようとする課題】しかしながら、このような措置は上記の特殊な環境を構築するための費用がかかり、また作業者也限定されるので生産性が低下するという問題がある。さらに、一般に組立部は、機種ごとに異なる工場に置かれることが多い。そのため、上記の特殊な環境の構築はそれぞれの工場で必要となり、構築費用はますます増大してしまうという問題がある。

【0011】本発明は、特殊な環境の構築費用の増大や生産性の低下を防ぎ、機器固有秘密情報を有する有料コンテンツ再生機器を製造する製造方法、有料コンテンツ再生機器に機器固有秘密情報とLSIとを供給する供給システムおよび前記製造方法において製造される有料コンテンツ再生機器を提供することを目的とする。

【0012】

【課題を解決するための手段】上記目的を達成する製造方法は、復号鍵を用いて復号処理を施す復号装置の製造方法であって、セキュリティが管理された状態において前記復号鍵を秘密に取得する取得ステップと、前記セキュリティが管理された状態において、取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して出力する変換情報出力ステップと、出力された前記変換情報を、前記復号装置に組み込まれるべ

き不揮発性メモリに書き込む書き込みステップと、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とが集積された1個の集積素子を含む前記復号装置を組み立てる組み立てステップとを含むことを特徴とする。

【0013】この構成によれば、復号鍵をそのまま使用せず、一旦暗号処理を施した暗号化復号鍵が、書き込みステップと組み立てステップとにおいて使用されている。それゆえこれらのステップは、セキュリティの管理された場所において実施する必要がない。また、素子内部にて復号処理を施された復号鍵は、素子の外部に出力されることがないので機密性は保持される。

【0014】したがって、書き込みステップと組み立てステップとを含む復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐ製造方法を提供することができる。また、上記目的を達成する供給システムは、復号装置に書き込まれる情報を供給する情報供給装置と、当該復号装置に組み込まれる集積素子を供給する集積素子供給装置とからなる供給システムであって、前記情報供給装置は、セキュリティの管理された状態で設けられ、前記復号装置において復号処理に用いられる復号鍵を秘密に取得する取得手段と、前記取得手段により取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して、当該変換情報を前記復号装置を組み立てる組立部に出力する変換情報出力手段とを備え、前記集積素子供給装置は、前記暗号化復号鍵に前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と、当該復号鍵を用いて復号処理を施す回路とが集積された1個の集積素子を製造する製造手段と、前記製造手段により製造された集積素子を前記組立部に供給する集積素子供給手段とを備えることを特徴とする。

【0015】この構成によれば、情報供給装置は、セキュリティの管理された場所に設けられ、復号鍵に一旦暗号処理を施して暗号化復号鍵を生成する。その暗号鍵復号鍵は変換情報に含められて組立部に供給される。したがって、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐ供給システムを提供することができる。

【0016】また、上記目的を達成する復号装置は、復号鍵を用いて復号処理を施す復号装置であって、前記復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれている不揮発性メモリと、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含む1個の集積素子とを備えることを特徴とする。

【0017】この構成によれば、復号鍵をそのまま扱わず、一旦暗号処理を施した暗号化復号鍵を扱うことで、装置の組み立て時に、セキュリティの管理された場所において実施する必要がない。また、素子内部にて復号処理を施された復号鍵は、素子の外部に出力されることがないので機密性は保持される。したがって、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐことができる。

【0018】

【発明の実施の形態】（実施の形態1）図1は本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造方法に関する実施の形態1の構成を示す図である。秘密情報発行部1は、機器製造の許可を受けた機器製造部2に機器固有秘密情報を発行して送付する。

【0019】機器製造部2は、機器固有秘密情報を有する有料コンテンツ再生機器を製造し、変換部3、組立部4およびLSI製造部5を備える。変換部3は、セキュリティの管理された場所で、機器固有秘密情報に対して所定の暗号処理を施して暗号化固有情報を生成する。生成された暗号化固有情報は組立部4に送付される。

【0020】ここで、セキュリティの管理された場所とは、施錠可能なドアと仕切りによって区切られた作業スペースのような、機密性の保持された場所を指す。また、所定の暗号処理としては、DES (Data Encryption Standard) 暗号の64ビット（パリティビット8ビットを含む）の秘密鍵を用いた暗号処理を用いる。なお、DESについては、例えば、岡本栄司著「暗号理論入門」（共立出版）に詳しく書かれている。

【0021】組立部4は、送付された暗号化固有情報を不揮発性メモリに書き込み、LSI製造部5で製造された暗号処理用LSIなどを組み立てて、有料コンテンツ再生機器を製造する。図2は有料コンテンツを再生する場合の不揮発性メモリと暗号処理用LSIとの構成を示す図である。

【0022】不揮発性メモリ6は、組立部4において暗号化固有情報が書き込まれ、暗号処理用LSI7と接続されて有料コンテンツ再生機器に組み込まれる。暗号処理用LSI7は、LSI製造部5において製造されたもので、秘密情報復号回路71、コンテンツ鍵復号回路72およびコンテンツ復号回路73を有し、機器固有秘密情報を復号鍵として送付される暗号化コンテンツ鍵データを復号化し、さらに当該コンテンツ鍵を用いて、暗号化コンテンツデータを復号化する。

【0023】秘密情報復号回路71は、変換部3において機器固有秘密情報に施した所定の暗号処理に対応する復号処理を行う回路である。これによって、暗号化固有情報は機器固有秘密情報に復号化される。具体的には、64ビット（パリティ8ビットを含む）の秘密鍵を用い

たDES暗号の復号処理を用い、秘密鍵は変換部3で用いられている暗号処理と同じものを用いる。

【0024】コンテンツ鍵復号回路72は、秘密情報復号回路71で復号化されて得た機器固有秘密情報を用いて、外部から入力される暗号化コンテンツ鍵データに対する復号処理を行う。コンテンツ復号回路73は、コンテンツ鍵復号回路72で復号化されたコンテンツ鍵を用いて、外部から入力される暗号化コンテンツデータを復号化してコンテンツデータを得る。

【0025】図3は本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造工程の手順を示す図である。次に実施の形態1における有料コンテンツ再生機器の製造工程の手順を図3を用いて説明する。秘密情報発行部1が、機器製造の許可を受けた機器製造部2に機器固有秘密情報を発行して送付する(ステップ:S11)。

【0026】変換部3が、セキュリティの管理された場所で、送付された機器固有秘密情報を秘密に取得し(ステップ:S12)、機器固有秘密情報に対して所定の暗号処理を施して暗号化固有情報を生成する(ステップ:S13)。生成された暗号化固有情報は組立部4に送付される。組立部4が、送付された暗号化固有情報を不揮発性メモリに書き込み(ステップ:S14)、LSI製造部5で製造された暗号処理用LSIなどを組み立てて(ステップ:S15)、有料コンテンツ再生機器を製造する。

【0027】実施の形態1では、変換部3において変換された暗号化固有情報は、秘密情報復号回路71において元の機器固有秘密情報に復号化され、コンテンツ鍵復号回路72に入力される。したがって、暗号化コンテンツ鍵データの復号処理は、秘密情報発行部1で発行された機器固有秘密情報と同じものを用いて行われるので、以降のコンテンツ復号処理は正しく行われる。

【0028】また、機器固有秘密情報は、暗号化固有情報の状態で組立部4に送付される。暗号化固有情報は、所定の暗号処理により変換された後のデータであるから、機器固有秘密情報のように機密性を保持する必要はない。したがって、組立部4において、不揮発性メモリに書き込み、及び組み立て作業の際に機密性を保持するための特殊な環境を構築する必要がない。即ち、組立部4における特殊な環境の構築費用の増大や生産性の低下は生じない。

【0029】(実施の形態2)図4は本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造方法に関する実施の形態2の構成を示す図である。実施の形態2では、変換部10において所定の暗号処理が複数種類の暗号処理から選択されたものであることが特徴となっており、その他については実施の形態1と同様であるので説明を省略する。

【0030】秘密情報発行部8は、機器製造部9に機器

固有秘密情報を送付する。機器製造部9は、変換部10、組立部11およびLSI製造部12を備える。変換部10は、セキュリティの管理された場所において、機器固有秘密情報に複数種類の暗号処理のいずれかの暗号処理を施して暗号化固有情報を生成する。変換部10は、さらに、いずれの変換を選んだかを示すパラメータ情報と暗号化固有情報とを組立部11に送付する。具体的には、複数種類の暗号処理は、生成された64ビットの秘密鍵を16種類選んだDES暗号の暗号処理とし、それぞれの秘密鍵に1から16までの番号を割り当て、この番号をパラメータ情報とする。

【0031】組立部11は、変換部10から送付された暗号化固有情報とパラメータ情報とを不揮発性メモリに書き込み、LSI製造部12で製造された暗号処理用LSIなどを組み立てて、有料コンテンツ再生機器を製造する。図5は有料コンテンツを再生する場合の不揮発性メモリと暗号処理用LSIとの構成を示す図である。

【0032】不揮発性メモリ13は、暗号化固有情報とパラメータ情報とが書き込まれ、暗号処理用LSI14と接続されて有料コンテンツ再生機器に組み込まれる。暗号処理用LSI14は、LSI製造部12において製造されたもので、パラメータ記憶手段141、秘密情報復号回路142、コンテンツ鍵復号回路143及びコンテンツ復号回路144を有する。

【0033】パラメータ記憶手段141は、変換部10が有する複数種類の暗号処理のそれぞれに対応したパラメータ情報を記憶している。具体的には、先ほど述べた16種類の秘密鍵を用いたDES暗号の復号処理と1から16の番号とを対応させた形で記録している。秘密情報復号回路142は、不揮発性メモリ13から暗号化固有情報とパラメータ情報とを読み取り、パラメータ情報を元に選んだ復号処理を暗号化固有情報に施すことによって、機器固有秘密情報を得る。

【0034】図6は本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造工程の手順を示す図である。次に実施の形態2における有料コンテンツ再生機器の製造工程の手順を図6を用いて説明する。秘密情報発行部8が、機器製造の許可を受けた機器製造部9に機器固有秘密情報を発行して送付する(ステップ:S21)。

【0035】変換部10が、セキュリティの管理された場所で、送付された機器固有秘密情報を秘密に取得する(ステップ:S22)。さらに変換部10が、複数種類の暗号処理の中からいずれかを選択し(ステップ:S23)、機器固有秘密情報に対して選択された暗号処理を施して暗号化固有情報を生成する(ステップ:S24)。その後、選択された所定の暗号処理を示すパラメータ情報と生成された暗号化固有情報とが、組立部11に送付される。

【0036】組立部11が、送付されたパラメータ情報

と暗号化固有情報とを不揮発性メモリ 13 に書き込み（ステップ：S25）、LSI 製造部 12 で製造された暗号処理用 LSI などを組み立てて（ステップ：S26）、有料コンテンツ再生機器を製造する。実施の形態 2 においても、実施の形態 1 と同様、機密性を保持する必要のある機器固有秘密情報は、暗号化固有情報に変換されて組立部 11 に送付されるので、組立部 11 において機密性を保持するための特殊な環境の必要がない。したがって、特殊な環境を構築する費用の増大や生産性の低下は生じない。また、機器固有秘密情報の暗号処理が固定的でなく、同じ機器固有秘密情報であっても選択する暗号処理を変えることで暗号化固有情報を異ならせることができるので、実施の形態 1 よりも機器固有秘密情報の機密性が向上している。

【0037】なお、実施の形態 1 において、変換部 3 において用いる所定の暗号処理は、64 ビットの秘密鍵を用いた DES 暗号処理を用い、その暗号処理に対応する復号処理は、同じ固定鍵を用いた DES 復号処理を用いているが、これは暗号処理と復号処理との関係にある変換であれば何でもよい。同様に、実施の形態 2 において、変換部 10 において用いる複数種類の所定の暗号処理は、16 種類の 64 ビットの秘密鍵を用いた DES 暗号処理を用いているが、これも暗号処理と復号処理との関係にある変換であれば何でもよい。また、暗号処理の個数は 16 個に限定されないことはいうまでもない。

【0038】さらに、実施の形態 2 において、変換部 10 において用いる複数種類の暗号処理は、16 種類の秘密鍵を用いた DES 暗号変換を用いているが、この 16 種類の秘密鍵は、予め決めた固定の値とする必要はなく、例えば、LSI のロットが変わる毎に異なる鍵を用いてもよい。また、実施の形態 1 および実施の形態 2 において、機器製造部にある組立部は、1 つだけの構成となっているが、これは複数であってもよい。さらに、変換部や LSI 製造部も 1 つだけである必要はなく、これらも複数であってもよい。

【0039】また、実施の形態 1 および実施の形態 2 において、機器製造部に交換部、組立部および LSI 製造部がある構成になっているが、この構成に限られるものではない。例えば、機器の組み立てを行う組立会社と LSI 製造を行う LSI 製造会社との 2 つの会社に分かれている場合には、LSI 製造会社に変換部と LSI 製造部とがあり、LSI 製造会社は暗号化固有情報と暗号処理用 LSI とを組立会社へ送付し、組立会社において、暗号化固有情報を不揮発性メモリに書き込み、暗号処理用 LSI などと組み立てるという構成でもよい。

【0040】この場合には、LSI 製造会社から送付される暗号化固有情報は機密性を保持する必要がないので、組立会社では、機密性を保持する特殊な環境を構築せずに組立が行える。また、このとき LSI 製造会社や組立会社は複数であってもよい。なお、実施の形態 1 およ

び実施の形態 2 において、不揮発性メモリは、いわゆる ROM だけのことを指すのではなく、ハードロジック、印刷パターン、ヒューズなどの様にデータを蓄える場合に揮発性のものではないことを指す。

【0041】

【発明の効果】本発明に係る製造方法は、復号鍵を用いて復号処理を施す復号装置の製造方法であって、セキュリティが管理された状態において、前記復号鍵を秘密に取得する取得ステップと、前記セキュリティが管理された状態において、取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して出力する変換情報出力ステップと、出力された前記変換情報を、前記復号装置に組み込まれるべき不揮発性メモリに書き込む書き込みステップと、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とが集積された 1 個の集積素子を含む前記復号装置を組み立てる組み立てステップとを含むことを特徴とする。

【0042】この構成によれば、復号鍵をそのまま使用せず、一旦暗号処理を施した暗号化復号鍵が、書き込みステップと組み立てステップとにおいて使用されている。それゆえこれらのステップは、セキュリティの管理された場所において実施する必要がない。また、素子内部にて復号処理を施された復号鍵は、素子の外部に出力されることがないので機密性は保持される。

【0043】したがって、書き込みステップと組み立てステップとを含む復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐ製造方法を提供することができる。また、前記書き込みステップは、前記セキュリティが管理された状態よりもセキュリティレベルの低い状態で実施されてもよい。

【0044】このように機密性の必要なところと不必要なところとを差別化することで、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とがない製造方法を実現することができる。また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記変換情報出力ステップは、所定の固定値の秘密鍵を用いて前記復号鍵に暗号処理を施すこととしてもよい。

【0045】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、前記変換情報出力ステップは、複数種類の暗号処理から 1 個を選択して、前記所定の暗号処理とする選択サブステップと、前記選択サブステップにより選択された前記所定の暗号処理を示す選択情報を生成する選択情報生成サブステップと、前記復号鍵に前記所定の暗号処理を施して

暗号化復号鍵を生成する暗号処理サブステップと、前記暗号化復号鍵と前記選択情報とを含む変換情報を生成する変換情報生成サブステップとを含み、前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むこととしてもよい。

【0046】このように、復号鍵は複数種類の暗号処理のいずれか1個の暗号処理を施される。したがって、暗号処理が1種類だけの場合に比べて復号鍵の機密性を高めることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【0047】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記選択サブステップは、複数の秘密鍵から1個の秘密鍵を選択し、前記選択情報生成サブステップは、選択された前記秘密鍵を示す選択情報を生成し、前記暗号処理サブステップは、選択された前記秘密鍵を用いて、前記復号鍵に暗号処理を施して暗号化復号鍵を生成し、前記変換情報生成サブステップは、前記暗号化復号鍵と前記選択情報とを含む変換情報を生成し、前記特定回路は、前記選択情報に基づいて、選択された前記秘密鍵を特定することとしてもよい。

【0048】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【0049】また、前記変換情報出力ステップは、さらに、前記複数の秘密鍵を生成する鍵生成サブステップを含み、前記選択サブステップは、当該鍵生成サブステップにより生成された前記複数の秘密鍵から1個の前記秘密鍵を選択することとしてもよい。これによって複数の秘密鍵を生成することができる。また、秘密鍵を変更することができるので、機密性が向上する。

【0050】また、前記取得ステップは、復号装置毎に固有の復号鍵を取得することとしてもよい。このように、復号鍵は復号装置毎に個々に割り当てられ、復号装置と復号鍵とを1対1で対応させることができる。また、本発明に係る供給システムは、復号装置に書き込まれる情報を供給する情報供給装置と、当該復号装置に組み込まれる集積素子を供給する集積素子供給装置とからなる供給システムであって、前記情報供給装置は、セキュリティの管理された状態で設けられ、前記復号装置において復号処理に用いられる復号鍵を秘密に取得する取得手段と、前記取得手段により取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して、当該変換情報を前記復号装置を組み立てる組立部に出力する変換情報出力手段とを備え、前記集積素

子供給装置は、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と、当該復号鍵を用いて復号処理を施す回路とが集積された1個の集積素子を製造する製造手段と、前記製造手段により製造された集積素子を前記組立部に供給する集積素子供給手段とを備えることを特徴とする。

【0051】この構成によれば、情報供給装置は、セキュリティの管理された場所に設けられ、復号鍵に一旦暗号処理を施して暗号化復号鍵を生成する。その暗号化復号鍵は変換情報に含められて組立部に供給される。したがって、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐ供給システムを提供することができる。

【0052】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記変換情報出力手段は、所定の固定値の秘密鍵を用いて前記復号鍵に暗号処理を施すこととしてもよい。このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、前記変換情報出力手段は、複数種類の暗号処理から1個を選択して、前記所定の暗号処理とする選択手段と、前記選択手段により選択された前記所定の暗号処理を示す選択情報を生成する選択情報生成手段と、前記復号鍵に前記所定の暗号処理を施して暗号化復号鍵を生成する暗号処理手段と、前記暗号化復号鍵と前記選択手段とを含む変換情報を生成する変換情報生成手段とを含み、前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むこととしてもよい。

【0053】このように、復号鍵は複数種類の暗号処理のいずれか1個の暗号処理を施される。したがって、暗号処理が1種類だけの場合に比べて復号鍵の機密性を高めることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【0054】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記選択手段は、複数の秘密鍵から1個の秘密鍵を選択し、前記選択情報生成手段は、選択された前記秘密鍵を示す選択情報を生成し、前記暗号処理手段は、選択された前記秘密鍵を用いて、前記復号鍵に暗号処理を施して暗号化復号鍵を生成し、前記変換情報生成手段は、前記暗号化復号鍵と前記選択手段とを含む変換情報を生成し、前記特定回路は、前記選択情報に基づいて、選択された前記秘密鍵を特定することとしてもよい。

【0055】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、選択

情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【0056】また、前記変換情報出力手段は、さらに、前記複数の秘密鍵を生成する鍵生成手段を含み、前記選択手段は、当該鍵生成手段により生成された前記複数の秘密鍵から1個の前記秘密鍵を選択することとしてもよい。これによって複数の秘密鍵を生成することができる。また、秘密鍵を変更することができるので、機密性が向上する。

【0057】また、前記取得手段は、復号装置毎に固有の復号鍵を取得することとしてもよい。このように、復号鍵は復号装置毎に個々に割り当てられ、復号装置と復号鍵とを1対1で対応させることができる。また、本発明に係る復号装置は、復号鍵を用いて復号処理を施す復号装置であって、前記復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれている不揮発性メモリと、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含む1個の集積素子とを備えることを特徴とする。

【0058】この構成によれば、復号鍵をそのまま扱わず、一旦暗号処理を施した暗号化復号鍵を扱うことで、装置の組み立て時に、セキュリティの管理された場所において実施する必要がない。また、素子内部にて復号処理を施された復号鍵は、素子の外部に出力されることがないので機密性は保持される。したがって、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐことができる。

【0059】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記不揮発性メモリは、所定の固定値の秘密鍵を用いて、前記復号鍵に秘密鍵暗号方式の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれており、前記集積素子は、前記暗号化復号鍵に、前記秘密鍵を用いて復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含むこととしてもよい。

【0060】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、前記不揮発性メモリは、複数種類の暗号処理から1個を選択して前記所定の暗号処理とし、選択された前記所定の暗号処理を示す選択情報と前記暗号化復号鍵とを含む変換情報が書き込まれており、前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むこととしてもよい。

【0061】このように、復号鍵は複数種類の暗号処理のいずれか1個の暗号処理を施される。したがって、暗号処理が1種類だけの場合に比べて復号鍵の機密性を高

めることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【0062】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記不揮発性メモリは、複数の秘密鍵から1個の秘密鍵を選択し、選択された前記秘密鍵を示す選択情報と、前記秘密鍵を用いて秘密鍵暗号方式の暗号処理を施した暗号化復号鍵とを含む変換情報が書き込まれており、前記集積素子は、前記選択情報に基づいて、選択された前記秘密鍵を特定する前記特定回路を含むこととしてもよい。

【0063】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【0064】また、前記不揮発性メモリは、復号装置毎に固有の復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれていることとしてもよい。このように、復号鍵は復号装置毎に個々に割り当てられ、復号装置と復号鍵とを1対1で対応させることができる。

【図面の簡単な説明】

【図1】本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造方法に関する実施の形態1の構成を示す図である。

【図2】有料コンテンツを再生する場合の不揮発性メモリと暗号処理用LSIとの構成を示す図である。

【図3】本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造工程の手順を示す図である。

【図4】本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造方法に関する実施の形態2の構成を示す図である。

【図5】有料コンテンツを再生する場合の不揮発性メモリと暗号処理用LSIとの構成を示す図である。

【図6】本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造工程の手順を示す図である。

【図7】記録媒体を利用した有料コンテンツ配布方式の構成を示す図である。

【図8】インターネットや放送網を利用した有料コンテンツ配信方式の構成を示す図である。

【図9】暗号処理用LSI25の内部構成を示す図である。

【図10】不揮発性メモリと暗号処理用LSIとを備える有料コンテンツ再生機器の製造方法に関する従来の構成を示す図である。

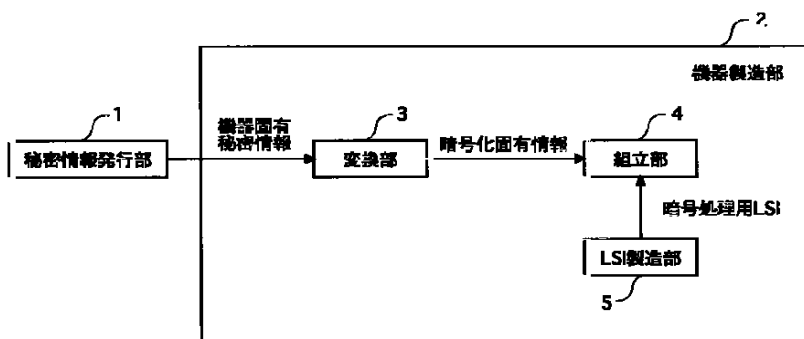
【符号の説明】

1、8

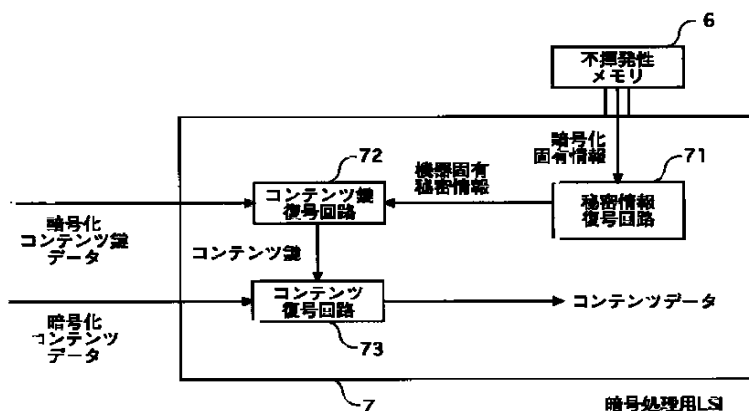
秘密情報発行部

2、9	機器製造部	7、14	暗号処理用LSI
3、10	変換部	71、142	秘密情報復号回路
4、11	組立部	72、143	コンテンツ鍵復号回路
5、12	LSI製造部	73、144	コンテンツ復号回路
6、13	不揮発性メモリ	141	パラメータ記憶手段

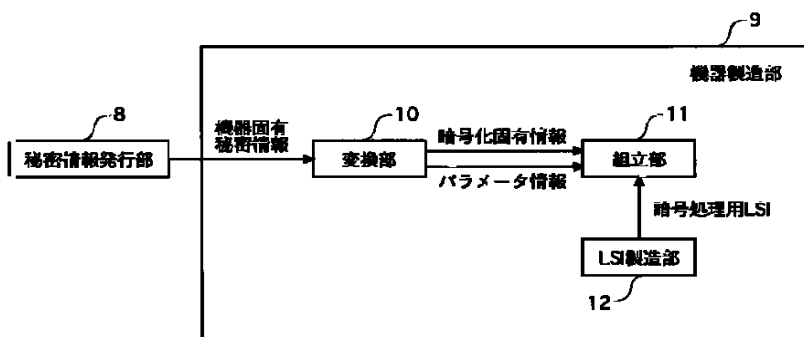
【図1】



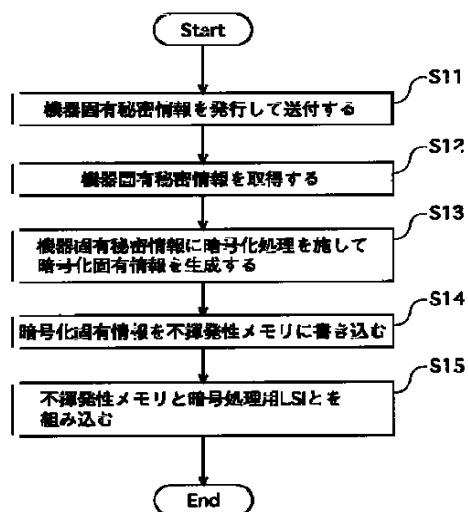
【図2】



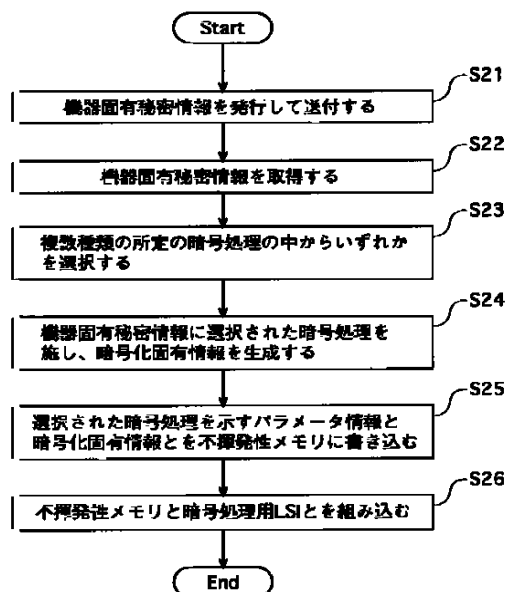
【図4】



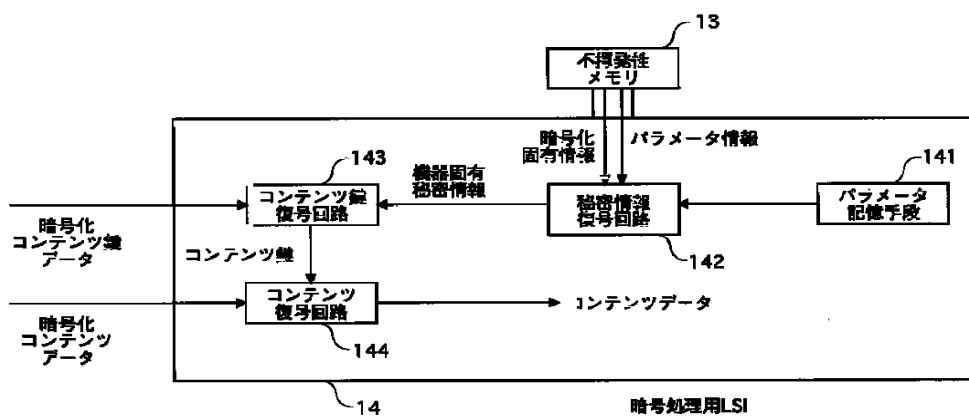
【図3】



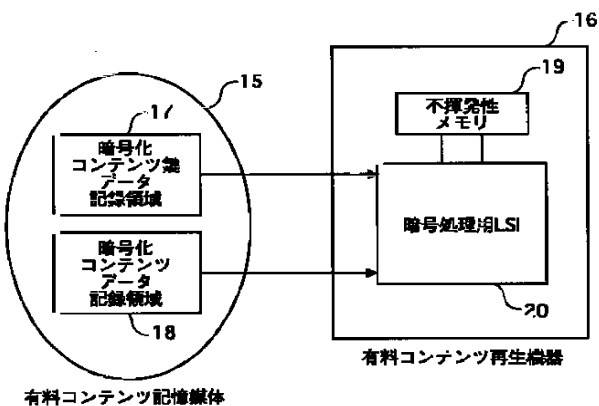
【図6】



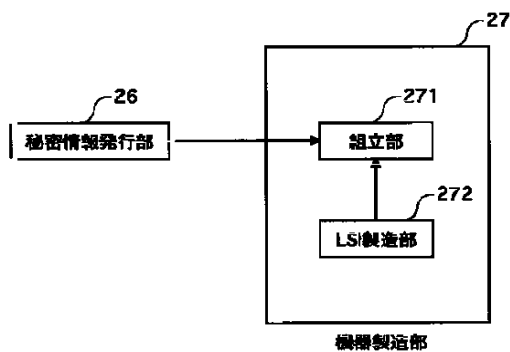
【図5】



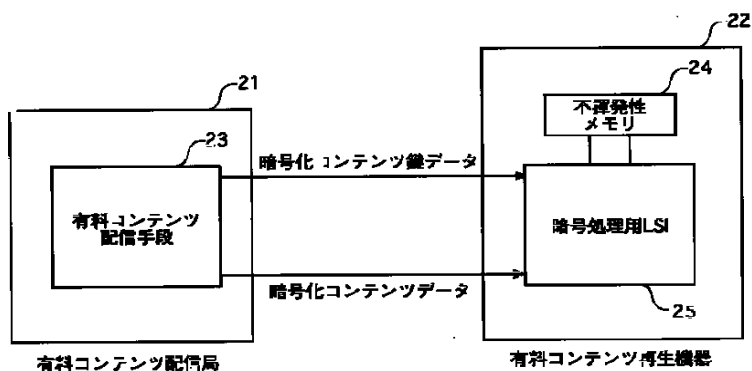
【図7】



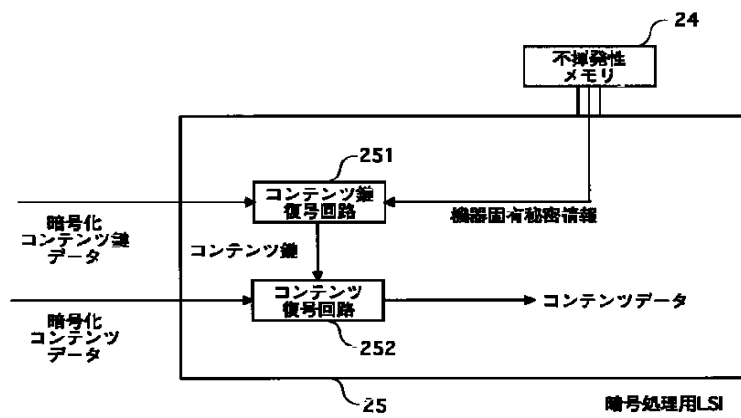
【図10】



【図8】



【図9】



フロントページの続き

(72)発明者 井上 信治
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

Fターム(参考) 5B017 AA03 AA06 BA07 BB09 BB10
CA05 CA12
5J104 AA12 AA16 EA04 EA26 JA03
KA14 NA02 NA27 NA37 NA39
NA42